UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE NEW YORK TIMES COMPANY, NICHOLAS CONFESSORE, and GABRIEL DANCE, Plaintiffs, - against - FEDERAL COMMUNICATIONS COMMISSION, Defendant.	:	18 Civ. 8607 (LGS)

MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT'S MOTION FOR SUMMARY JUDGMENT AND IN SUPPORT OF PLAINTIFFS' CROSS-MOTION FOR SUMMARY JUDGMENT

David E. McCraw, Esq.
Al-Amyn Sumar, Esq.
The New York Times Company
Legal Department
620 Eighth Avenue
New York, NY 10018
Phone: (212) 556-4031
Fax: (212) 556-4634
mccraw@nytimes.com

John D. Clopper, Esq.
Clopper Law PC
43 West 43rd Street, Suite 95
New York, NY 10036
Phone: (347) 752-7757
jclopper@clopperlaw.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules & Regulations

Other Authorities

Plaintiffs The New York Times Company, Nicholas Confessore, and Gabriel Dance (collectively, "The Times") respectfully submit this memorandum of law in opposition to the motion for summary judgment by Defendant Federal Communications Commission ("FCC") and in support of their cross-motion for summary judgment on their Complaint brought under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552.

PRELIMINARY STATEMENT

In 2017, the FCC undertook a controversial initiative to revoke the "net neutrality" rules enacted under the Obama administration. We now know that the agency's notice-and-comment process – one of the benchmarks of democracy in administrative rule-making – was hijacked by Russians and others using automation to disrupt the system, creating the lie that millions of citizens were demanding that action be taken on net neutrality. The FOIA request that is the subject of this litigation represents an attempt by The Times to get at vital information that will help the public know more about the illicit – and apparently successful – effort to corrupt the notice-and-comment process.

Since June 22, 2017, reporters at *The New York Times* have been asking the FCC to release server log records containing the needed information. In essence, the reporters seek information about the computers from which the submissions originated. That information would help establish whether the comments were coming from a small number of computers, even though they appeared to be sent in by individual citizens – information that would help the public know whether multiple bad actors were involved, where they were located, and how concentrated their disruption efforts were. For over a year, The Times worked with the FCC to narrow its request in an effort to obtain the information that its reporters required. That effort was met by delay and obfuscation. Most incredibly: The FCC claimed for months that it did not

have the requested information in a single server log – only to reverse course in its brief to this Court, when it acknowledged it did in fact have such a log.

The Times seeks the release of that log. Though the FCC claims that the log reflects comments made in all notice-and-comment proceedings in a set time period, The Times believes that the agency can easily identify the entries pertaining to the net neutrality proceeding and eliminate the others. But if the Court concludes that the FCC is not required to undertake that operation, The Times is prepared to accept the entire log.

Beyond that issue of segregating the information related to net neutrality, the only remaining dispute between the parties is whether the information can be withheld under Exemption 6 of FOIA, which can be invoked to protect "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." Information identifying the computer addresses and web browsers used by the commenters does not infringe on anyone's privacy, and the FCC offers only fanciful and speculative arguments about how the information might be misused. On the other hand, the public importance of the information is plain: Release of the log will permit reporters to determine – to a greater degree of certainty than possible based on currently public information – whether the FCC's handling of this important public policy matter was unduly affected by fraud, and, quite possibly, deliberate interference in the United States' established legal framework for public participation in agency rulemaking.

STATEMENT OF FACTS

The Rulemaking to Repeal "Net Neutrality"

On May 18, 2017, the FCC adopted a notice of proposed rulemaking titled "Restoring Internet Freedom," with docket number 17-108. *See* FCC 17-60, *Notice of Proposed*

Rulemaking, https://bit.ly/2TPWXdA. The controversial proposal sought to repeal rules enacted in 2015 under the Obama Administration that gave legal force to "net neutrality," *i.e.*, the principle that internet service providers must provide "equal access to all web content." *See* Keith Collins, *Net Neutrality Has Officially Been Repealed. Here's How That Could Affect You.*, N.Y. Times (June 11, 2018), https://nyti.ms/2l2dEDB.[1] The FCC's proposal was immediately controversial and subject to vigorous public debate. *See, e.g.*, Cecilia Kang, *F.C.C. Chairman Pushes Sweeping Changes to Net Neutrality Rules*, N.Y. Times (Apr. 26, 2017), https://nyti.ms/2q6X72I. Critics contended that the proposal would undermine the open internet and open the door to service providers' establishing fast lanes for consumers and companies who pay premiums and a slow lane for those who do not. *See id.*

Members of the public were allowed to submit comments to the FCC in the spring and summer of 2017. *See* Paul Hitlin and Skye Toor, *Public Comments to the Federal Communications Commission About Net Neutrality Contain Many Inaccuracies and Duplicates*, Pew Research Center (Nov. 29, 2017), https://pewrsr.ch/2AiqeFR ("Pew Net Neutrality Report"). Some 21.7 million comments were submitted electronically to the FCC by the close of the comment period. *Id.* The FCC ultimately enacted the proposed changes – thereby repealing the net neutrality rules – in December 2017. Cecilia Kang, *F.C.C. Repeals Net Neutrality Rules*, N.Y. Times (Dec. 14, 2017), https://nyti.ms/2COjIcm.

[1] The Congressional Research Service notes that while there is "no single accepted definition of 'net neutrality,'" it is commonly accepted that "any such definition should include the general principles that owners of the networks that compose and provide access to the internet should not control how consumers lawfully use that network, and they should not be able to discriminate against content provider access to that network." Congressional Research Service, *The Net Neutrality Debate: Access to Broadband Networks* (updated Mar. 21, 2019), https://bit.ly/2G7VREn, at 1.

The FCC's Handling of the Notice-and-Comment Period

The FCC has already come under scrutiny for misleading the public about early problems in the notice-and comment process. On May 7, 2017, the FCC's Electronic Comment Filing System ("ECFS") experienced a temporary "disruption in system availability" (*i.e.*, a website crash). *See* FCC Office of Inspector General, *Memorandum* (June 20, 2018) ("OIG Report"), https://bit.ly/2Bak4f1, at 2. The next day, the FCC's Chief Information Officer issued a press release attributing the system disruptions to "multiple denial-of-service attacks" on the comment system.[2] *Id.* He said the perpetrators of the attacks "were not attempting to file comments themselves; rather they made it difficult for legitimate commenters to access and file with the FCC." *Id.* As it turns out, that story was false. An investigation by the FCC's Office of Inspector General ("OIG") revealed that the disruptions were caused not by a DDoS attack, but instead by the huge influx of comments following the airing of an HBO episode of "Last Week Tonight with John Oliver" on May 7, in which host John Oliver urged his viewers to file comments on ECFS opposing the proposal to repeal net neutrality. *Id.* at 7.[3] In an August 14, 2018, letter to FCC Chairman Ajit Pai, several members of Congress wrote that they were "deeply disturbed" by the OIG Report and "troubl[ed] that [Pai] allowed the public myth created by the FCC to persist and [his] misrepresentations to remain uncorrected for over a year." Dell Cameron, *Ajit*

[2] "Distributed Denial of Service (DDoS) attacks flood their target with requests, consuming the target's bandwidth and/or overloading the capacity of the host server, resulting in service outages." Catherine A. Theohary and Anne I. Harrington, Congressional Research Service, *Cyber Operations in DOD Policy and Plans: Issues for Congress* (Jan. 5, 2015), https://bit.ly/2JXWNS1, at 4.

[3] The OIG's report also blamed "high volume traffic resulting from system design issues." OIG Report at 7.

Pai Is Getting Grilled for Misleading Congress Over Imaginary Cyberattacks, Gizmodo (Aug. 14, 2018), https://bit.ly/2I5Ziir.

Evidence of Automated Comments, Russian Interference, and Fraud

After the comment period ended, the press, academic researchers, and other governmental entities began multiple investigations into the FCC's handling of the rulemaking. Thus far, these investigations have revealed that the public comment process in the net neutrality rulemaking was tainted by fraud, including comments from automated bots and comments submitted from fraudulent Russian email accounts. For instance:

- A 2017 report by the Pew Research Center found that 57% of the comments were submitted using duplicate or temporary email addresses, and that 94% of the comments were submitted multiple times – in some instances, "hundreds of thousands of times." Pew Net Neutrality Report. The report also found that on nine different occasions, "more than 75,000 comments were submitted at the very same second – often including identical or highly similar comments." *Id.*

- A separate analysis by a researcher at Stanford University found that the unique comments submitted – around 800,000 in total – were overwhelmingly in favor of net neutrality. Kaleigh Rogers, *99.7 Percent of Unique FCC Comments Favored Net Neutrality*, Motherboard (Oct. 15, 2018), https://bit.ly/2EmHJu4.

- A cyber-intelligence firm found that the same network of email addresses used by Russians to spread disinformation on social media during the 2016 presidential campaign was used to post comments on ECFS. *See generally* GroupSense, SHARK20385 (July 24, 2018), https://bit.ly/2OE9q21.[4]

The revelations that millions of comments were fraudulent – submitted under the names of other people, living or dead – has also prompted investigations by the FBI, the Attorney

[4] The FCC has publicly accepted that many of the comments were fake and of Russian origin. In a statement attached to the FCC's denial of The Times's administrative appeal, *see infra*, Chairman Pai acknowledged that half a million comments were "submitted from Russian e-mail addresses" and that nearly eight million comments were "filed by e-mail addresses from e-mail domains associated with FakeMailGenerator.com." *See* FCC 18-156, *Memorandum Opinion and Order* (Dec. 3, 2018), https://bit.ly/2HPvBTv ("FCC 18-156") at 13 (statement of Chairman Ajit Pai).

General of the State of New York, and the U.S. Government Accountability Office. *See* Jon Brodkin, *Report: FBI Opens Criminal Investigation Into Net Neutrality Comment Fraud*, Ars Technica (Dec. 10, 2018), https://bit.ly/2OFFN1t; Nicholas Confessore, *New York Attorney General Expands Inquiry Into Net Neutrality Comments*, N.Y. Times (Oct. 16, 2018), https://nyti.ms/2AeWdsc; Devin Coldewey, *The GAO Will Investigate Potential Fraud In The FCC's Net Neutrality Comments… In 5 Months*, TechCrunch (Jan. 23, 2018), http://tcrn.ch/2DGsQBD.

The FOIA Request and Administrative Proceedings

On behalf of The New York Times Company and fellow reporter Gabriel Dance, Plaintiff Nicholas Confessore submitted a Freedom of Information Act ("FOIA") request (the "Request") to the FCC on June 22, 2017. *See* Dkt. 24, Declaration of Erik Scheibert ("Scheibert Decl.") Ex. A. The Request sought web server logs[5] for all comments submitted to the FCC in docket 17-108 for a portion of the comment period – between April 26 and June 7, 2017 – including dates and time stamps, IP addresses, and browser information (known as "User Agent" information). *Id.*[6]

The FCC's declarant provides the tortured history of how the Request was handled. We need not repeat that narrative here. The simple story line is this: The Times attempted to work

[5] As the FCC notes, "[s]erver logs are files that a server automatically generates when it or another system element performs its activities." Scheibert Decl. ¶ 16.

[6] The Request read, in relevant part: "Please provide the web server logs for comments submitted for Federal Communications Commission docket No. 17-108 between 4/26/17 and 6/7/2017. I would like the logs for requests submitted via both to https://www.fcc.gov/ecfs/filings/ and any submissions through the FCC's API (application programming interface). For each comment, please include the following information: 1) Server logs for both GET and POST requests 2) The date/time stamp of each request 3) The full query including query strings 4) The IP address of the client making the request 5) The browser USE RAGE NT 6) The following headers when available: Accept, Accept-Encoding, Accept-Language, Connection, Host, ONT, Upgrade-Insecure-Requests, Via, X-Forwarded-For." Scheibert Decl. Ex. A.

with the FCC to identify information that could be released. The Times amended and narrowed its Request four times. The FCC provided a shifting explanation for what records it had and why it could not or would not produce them. Ultimately, on August 31, 2018, more than a year after making the original Request, The Times limited its Request to two pieces of information: the originating IP addresses and User-Agent headers, with their respective time-stamps. *Id.* Ex. I. Based on the FCC's claim in April 2018 that the two pieces of information existed in different logs, The Times proposed a "find and replace" system under which the FCC would link the logs containing the IP addresses to those with the User-Agent header by inserting a unique identifier. *Id.* Exs. H, I.

This Lawsuit

Having received no response to its amended Request, The Times filed its Complaint on this case on September 20, 2018. Dkt. 1. The Times seeks both the requested records and the costs of this proceeding, including its attorneys' fees. *Id.*; *see* 5 U.S.C. § 552(a)(4)(E)(i).

After The Times filed this suit, the agency finally issued a denial of The Times's administrative appeal. *See generally* FCC 18-156. The agency said that the originating IP addresses fall within FOIA Exemption 6, which applies where disclosure would constitute a clearly unwarranted invasion of privacy. *Id.* at 4-7. The FCC also said that the logs are independently exempt pursuant to Exemption 7(E), which protects investigative techniques used in law enforcement. *Id.* at 7-9. The FCC went on to hold that the non-exempt material in the logs could not be reasonably segregated and released. *Id.* at 9-10. It also argued that The Times's proposed "find-and-replace" method for linking the separate sets of logs was effectively a request that the agency "create new records." *Id.* at 10-11. In a dissenting statement, FCC Commissioner Jessica Rosenworcel faulted the majority for "thwart[ing] investigative

journalism," "hiding what it knows about the fraud in our record," and "preventing an honest account of its many problems from seeing the light of day." *Id.* at 14.

When the FCC filed its motion for summary judgment on March 14, 2019 (Dkt. 22), its story shifted dramatically once again. It now said only Exemption 6 was at issue. More remarkably, the FCC's motion papers disclosed, for the first time, that the agency *does* have a single server log – what it calls the "API proxy server log" – that contains *both* a user's originating IP address and User-Agent header information. *See* Dkt. 23, Defendant's Memorandum of Law ("FCC Memo") at 12 n.2. The FCC offered no explanation for its failure to disclose the existence of the log in the year-long, back-and-forth negotiations with The Times about the Request.[7]

ARGUMENT

FOIA requires that government records be made available to the public unless a statutory exemption applies. 5 U.S.C. § 552(a)(3)(A), (b)(1)-(9). "The basic purpose of FOIA reflected a general philosophy of full agency disclosure," and government agency records may be withheld only if they fall within one of the nine statutory exemptions. *Bloomberg, L.P. v. Bd. of Governors of the Fed. Reserve Sys.*, 601 F.3d 143, 147 (2d Cir. 2010) (quoting *Dep't of Air Force v. Rose*, 425 U.S. 352, 360-61 (1976)) (alterations omitted). In light of this purpose, "FOIA exemptions are to be construed narrowly." *Assoc. Press v. Dep't of Def.*, 554 F.3d 274,

[7] In light of the newly disclosed information,, The Times has agreed to narrow the Request to the API proxy server log (*see* Scheibert Decl. ¶ 29), reflecting entries generated between April 26, 2017 and June 7, 2017. The Times agrees that the FCC may limit its response to entries in the API proxy server log reflecting requests to submit comments (known as "POST" requests) and may segregate and redact entries reflecting requests to download comments (known as "GET" requests). The Times also agrees that, for purposes of entries reflecting POST requests, the FCC may limit its response to the following three types of information: timestamps, originating IP addresses, and User-Agent headers.

283 (2d Cir. 2009). There is a "strong presumption in favor of disclosure [that] places the burden on the agency to justify the withholding of any requested documents.'" *Id.* (quoting *Dep't of State v. Ray*, 502 U.S. 164, 173 (1991)) (internal marks omitted).

FOIA litigation is typically resolved on summary judgment. *See, e.g.*, *Carney v. Dep't of Justice*, 19 F.3d 807, 812 (2d Cir. 1994). In a FOIA case, as in other litigation, summary judgment is properly granted when there is no genuine issue as to any material fact and the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a); *Bryant v. Maffuci*, 923 F.2d 979, 982 (2d Cir. 1991).[8] Under FOIA, the agency bears the burden of demonstrating that a particular exemption applies, and doubts are resolved in favor of disclosure. *See Am. Civil Liberties Union v. Dep't of Def.*, 543 F.3d 59, 66 (2d Cir. 2008). Failure to meet that burden requires disclosure of the requested documents. *See Nat'l Council of La Raza v. Dep't of Justice*, 411 F.3d 350, 355 (2d Cir. 2005).

A Court reviews *de novo* an agency's decision to withhold information from the public. 5 U.S.C. § 552(a)(4)(B). As a result, the agency's decision as to the applicability of a given exemption is entitled to no judicial deference. *See Bloomberg*, 601 F.3d at 147. Although courts review reasonably detailed agency affidavits with a presumption of good faith, this primarily is for determining the need for further fact-finding. *See, e.g.*, *Wood v. Fed. Bureau of Investigation*, 432 F.3d 78, 85 (2d Cir. 2005); *see also Wilner v. Nat'l Sec. Agency*, 592 F.3d 60, 69 (2d Cir. 2009) (presumption does not replace *de novo* review by courts). "Conclusory assertions of privilege will not suffice to carry the government's burden of proof in defending FOIA cases."

[8] Neither The Times nor the FCC has not submitted a Local Rule 56.1 statement in accord with the practice in FOIA cases in this District. *See N.Y. Times Co. v. Dep't of Justice*, 872 F. Supp. 2d 309, 314 (S.D.N.Y. 2012) ("[T]he general rule in this Circuit is that in FOIA actions . . . Local Civil Rule 56.1 statements are not required.") (internal marks omitted).

Assadi v. Citizenship & Immigration Servs., 2015 WL 1500254, at *5 (S.D.N.Y. Mar. 31, 2015) (quoting *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 861 (D.C. Cir. 1980)) (internal marks omitted).

I.
EXEMPTION 6 DOES NOT APPLY TO THE IP ADDRESSES OR THE USER AGENT HEADER INFORMATION

Exemption 6 does not allow federal agencies to shield computer information about persons participating in notice-and-comment rulemaking when the public disclosure of that information involves a negligible privacy interest and will "shed[] light on an agency's performance of its statutory duties." *N.Y. Times Co. v. Dep't of Homeland Sec.*, 959 F. Supp. 2d 449, 454 (S.D.N.Y. 2013) (quoting *Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 773 (1989)). Exemption 6 is especially unavailable where, as here, commenters are specifically told that *all information* that they submit will be publicly available. *See, e.g.*, *People for the Am. Way Found. v. Nat'l Park. Serv.*, 503 F. Supp. 2d 284, 306 (D.D.C. 2007); *Alliance for the Wild Rockies v. Dep't of the Interior*, 53 F. Supp. 2d 32, 37 (D.D.C. 1999). Because the public interest in having a full and honest account of what happened during the net neutrality rulemaking is enormously important, and commenters' privacy interests in the log information is, at best, slight, Exemption 6 does not permit the FCC is withhold either the IP addresses or User-Agent headers in the logs.

Exemption 6 allows an agency to withhold records if disclosure "would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). To determine whether a disclosure would constitute a "clearly unwarranted invasion of personal privacy," the courts employ a balancing test, weighing "the private interest involved (namely, 'the individual's right

of privacy') against the public interest (namely, 'the basic purpose of the Freedom of Information Act,' which is 'to open agency action to the light of public scrutiny')." *Judicial Watch, Inc. v. Food & Drug Admin.*, 449 F.3d 141, 153 (D.C. Cir. 2006) (citation omitted); *Ray*, 502 U.S. at 172. "[U]nder Exemption 6, the presumption in favor of disclosure is as strong as can be found anywhere in the Act." *Multi Ag Media LLC v. Dep't of Agric.*, 515 F.3d 1224, 1227 (D.C. Cir. 2008) (citation and internal marks omitted); *see also Consumers' Checkbook Ctr. for the Study of Servs. v. Dep't of Health & Human Servs.*, 554 F.3d 1046, 1057 (D.C. Cir. 2009) ("[FOIA's] presumption favoring disclosure is at its zenith under Exemption 6.") (alteration, citation, and internal marks omitted). In balancing these interests, "the 'clearly unwarranted' language of Exemption 6 weights the scales in favor of disclosure," *Ripskis v. Dep't of Housing and Urban Dev.*, 746 F.2d 1, 3 (D.C. Cir. 1984); *see, e.g., Morley v. Cent. Intelligence Agency*, 508 F.3d 1108, 1127 (D.C. Cir. 2007) ("Exemption 6's requirement that disclosure be clearly unwarranted instructs us to tilt the balance (of disclosure interests against privacy interests) in favor of disclosure" and "creates a heavy burden" for an agency invoking Exemption 6) (internal marks omitted).

Preliminarily, it is important to understand that releasing IP addresses and User-Agent headers does not threaten the anonymity of commenters because commenters are not anonymous to begin with. The FCC argues, for example, that if IP addresses are released "there is a substantial possibility that the New York Times or any member of the public could match at least some of those IP addresses with individual commenters who made submissions to ECFS during the requested period, by looking up the public comments posted to FCC Docket No. 17-108." FCC Memo at 19. Setting aside the contradiction in the agency's briefing – The Times apparently *can* match comments in the net neutrality proceedings to specific entries in the API

proxy server log,[9] even though the agency is unable to do exactly that, *see infra* – this is also largely beside the point, for the simple reason that the identities of the commenters are already in the public domain. Rather, the relevant questions are (1) whether commenters – having voluntarily identified themselves by submitting comments on the public record – nonetheless retain a non-negligible privacy interest in the computer address from which the comment came and information about the computer's web browser, and (2) whether any such privacy interests outweigh the substantial public interest in release of the information.

The FCC argues that release of the API proxy server logs will threaten commenters' privacy because the log information can be linked to individuals and that the combined information could then be used by unidentified malicious actors to do some sort of online harm to the commenter's computer. FCC Memo at 19-20. The FCC's argument both dramatically overstates the possibility for privacy-interfering linkage of the information to individuals and is wildly speculative regarding the possible harms. IP addresses are generally not unique to devices used by individual internet consumers. Rather, most individuals connect their devices to the internet using a steadily changing series of IP addresses assigned by internet service providers. The process by which internet service providers rotate and reassign IP addresses is known as "dynamic IP addressing."[10] The practical consequence of dynamic IP addressing is simple: an

[9] The FCC claims that "the foundational premise" of The Times's Request is to match IP addresses to specific comments, and that if no such matching were possible "the requested information would be useless." FCC Memo at 19. It is wrong on both counts. The Times's statistical analysis is primarily geared at deducing broad patterns in the comments and commenters' IP addresses and User-Agent information. It does not depend at all on the ability to match comments to IP addresses.

[10] As one district court explained, "relatively few personal computer users have a specific, set IP address, called a 'static' address. Instead, many use their computers to connect to a network provided by their ISP, which uses a certain range of IP addresses—say, all of the numbers between 168.122.1.x to 168.122.100.x. The ISP assigns an address within its range to

internet-connected device's IP address today may not be its IP address tomorrow. And the IP address of a device used by a commenter in mid-2017 is almost certainly not its IP address in mid-2019. *See, e.g.*, *London-Sire*, 542 F. Supp. 2d at 160; *Call of the Wild Movie*, 770 F. Supp. 2d at 356. Similarly, the User-Agent information is not specifically and statically related to individuals over time. At most, the User-Agent information contained in the API Proxy server logs will reveal some very basic information—such as browser type and operating system—that was installed on a device in 2017.

The FCC has not shown that the possibility that this highly dated information could be at all useful to some malicious actor bent on doing harm to an individual commenter is more than remote and speculative. The Supreme Court has made clear that it takes more to qualify for protection under Exemption 6. *See Rose*, 425 U.S. at 380 n.19 ("The legislative history is clear that Exemption 6 was directed at threats to privacy interests more palpable than mere possibilities."); *Am. Civil Liberties Union*, 543 F.3d at 85-86 ("Even accepting [defendants'] argument that it may be 'possible' to identify the detainees in spite of the district court's redactions, or that there remains a 'chance' that the detainees could identify themselves . . . such

---

the user's computer for the user's session, allocating the numbers within its range on an as-needed basis. This process is known as 'dynamic' addressing." *London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153, 160 (D. Mass. 2008); *Call of the Wild Movie, LLC v. Does 1-1,062*, 770 F. Supp. 2d 332, 356 (D.D.C. 2011) ("Most consumer IP addresses are 'dynamic' as opposed to 'static.'") (citing *London-Sire*, 542 F. Supp. 2d at 160); *see also* Google, *Static v. Dynamic IP Addresses*, http://bit.ly/2P2H1UD ("When a device is assigned a *static* IP address, the address does not change. Most devices use *dynamic* IP addresses, which are assigned by the network when they connect and change over time."); PC Mag, *Definition of IP Address*, http://bit.ly/2WX45qC ("Network infrastructure devices such as servers, routers and firewalls are typically assigned permanent 'static' IP addresses. The client machines can also be assigned static IPs by a network administrator, but most often are automatically assigned 'dynamic' IP addresses via software in the router . . . . Internet service providers may change the IPs in the modems of their home users here and there, but business users must have consistent 'static' IPs for servers that face the public.").

speculation does not establish a privacy interest that surpasses a *de minimis* level for the purposes of a FOIA inquiry.").[11]

Apart from speculating about barely-conceivable harms from the unlikely misuse of outdated information by unidentified bad actors, the FCC's principal argument for invoking Exemption 6 is that commenters were not specifically told that IP addresses and User-Agent header information would be publicly released. FCC Memo at 20. Pointing to a disclosure statement provided to ECFS users, the FCC argues that "it does not give ECFS users *any* notice that their log data could be disclosed to third parties," *id.* (emphasis in original) and suggests that commenters are led to believe that only their names and postal addresses will be publicly available. *Id.*

The FCC is willfully misreading the privacy notice provided to commenters. Contrary to the FCC's suggestion, commenters are not led to believe that *only* their names and addresses will be released. Rather, commenters are expressly told that "all information submitted" will be publicly available. Specifically, the FCC's ECFS system alerts commenters that "[a]ll

[11] It is also possible – likely, in fact – that the some of the IP addresses and User-Agent information contained in the API proxy server logs are associated with devices owned not by individuals, but by organizations and other entities. Organizations and entities, as opposed to individuals, have no privacy interests cognizable under the FOIA. *See, e.g., Sims v. Cent. Intelligence Agency*, 642 F.2d 562, 572 n.47 (D.C. Cir. 1980) ("Exemption 6 is applicable only to individuals."); *Nat'l Parks and Conservation Ass'n v. Kleppe*, 547 F.2d 673, 686 n.44 (D.C. Cir. 1976) ("The sixth exemption has not been extended to protect the privacy interests of businesses or corporations."); *Hodes v Dep't of Housing and Urban Dev.*, 532 F. Supp. 2d 108, 119 (D.D.C. 2008) ("As a threshold matter, both Parties fail . . . to acknowledge that only individuals (not commercial entities) may possess protectible privacy interests under Exemption 6."); *Maydak v. Dep't of Justice*, 362 F. Supp. 2d 316, 324-25 (D.D.C. 2005) (stating that Exemption 6 applies "'only to individuals'" (quoting *Sims*, 642 F.2d at 572 n.47)). Accordingly, to the extent that the information in the API proxy server logs relates to comments submitted by organizations or other entities the information is categorically unprotected by Exemption 6. And to the extent the comments were submitted by individuals using devices owned by such entities, disclosure of the IP addresses and browser information do not implicate those individuals' privacy interests.

information submitted, including names and addresses, will be publicly available via the web." Scheibert Decl. ¶ 7.[12] Accordingly, commenters are on notice that the most revealing of personal information will be made public and that the information to be made public exceeds just name and address. No commenter could have understood the FCC to be saying that all information beyond name and address would be kept confidential.

In any event, even assuming that commenters retain some slight residual privacy interest in IP addresses and User-Agent header information, that interest is outweighed by the substantial public interest in understanding what happened during the net neutrality rulemaking and thereby "shed[] light on an agency's performance of its statutory duties." *Reporters Committee for Freedom of the Press,* 489 U.S. at 773. The public interest analysis turns on "the extent to which disclosure would serve the core purposes of the FOIA by contributing significantly to public understanding of the operations or activities of the government." *Nat'l Ass'n of Home Builders v. Norton,* 309 F.3d 26, 33 (D.C. Cir. 2002) (alterations and internal marks omitted); *see also Adelante Alabama Worker Ctr. v. Dep't of Homeland Sec.*, 2019 WL 1380334, at *16 (S.D.N.Y. Mar. 26, 2019) (holding Exemption 6 inapplicable because "the public interest in disclosure here is palpable, and the privacy interests at stake are, at most, slight . . . ."); *BuzzFeed, Inc. v. Dep't of Justice*, 2019 WL 1114864, at *9 (S.D.N.Y. Mar. 11, 2019) (ordering disclosure where public interest outweighs individuals' privacy rights).

[12] Similarly, the FCC's comment guide tells prospective commenters:

> Any comments that you submit to the FCC on a proposed rulemaking, petition, or other document for which public comment is requested will be made public, including any personally identifiable information you include in your submission. We may share non-personally identifiable information with others, including the public, in aggregated form, in partial or edited form, or verbatim.

FCC, *How to Comment on FCC Proceedings*, https://bit.ly/2A2PL5Q.

The public interest in getting and analyzing the contents of the API proxy server logs is considerable. Among other things, the logs will likely reveal the true extent of the fraud that infected the net neutrality rulemaking, including the extent to which cloud-based automated bots intervened in an important public debate. In the wake of Special Counsel's Robert Mueller's recent indictment of 13 Russian individuals and three Russian companies for interfering with U.S. elections and the U.S. political system, the public interest in understanding how these cloud-based automated bots are being used to influence an array of U.S. political activities—including the agency notice-and-comment process—is exceptionally high. Disclosure of the IP addresses and browser information will also provide clues as to where the purported commenters were geographically based – the United States, Russia, or elsewhere – and nature of the software they used to file comments. Put simply, the data can tell us who corrupted the notice-and comment process, and how they did it.

The FCC argues that there is no cognizable public interest at stake in this case because release of the API proxy server logs will shed no light on the FCC's performance of its statutory duties or increase the public's "understanding of the operations or activities of the government." FCC Memo at 21 (quoting *Long v. Office of Personnel Mgmt.*, 692 F.3d 185, 193 (2d Cir. 2012)). The FCC does not dispute that release of the API proxy server logs could shed light on the extent to which the net neutrality rulemaking was infected with fraud—and, possibly, foreign interference—but says that this "bears no relation" to the FCC's performance of its duties. *Id.* This is a remarkable and profoundly misguided argument. It should be obvious to the FCC that one of its principal statutory obligations is to ensure that it not allow public participation in the policy-making process to be overrun by bots and fake Russian-originated comments. Indeed, another district court has recognized exactly that: it ordered release of the email addresses

associated with transmittal of bulk comments in the net neutrality proceeding because disclosure would "reveal information at the heart of FOIA's purpose of illuminating agency action: It would clarify the extent to which the Commission succeeded—as it assured the American people it had—in managing a public-commenting process seemingly corrupted by dubious comments." *Prechtel v. Fed. Commc'ns Comm'n*, 330 F. Supp. 3d 320, 331 (D.D.C. 2018).[13] It is startling that the FCC does not appear to share that view.

FCC Commissioner Rosenworcel recently explained the deeply troubling problems that have arisen in the agency notice-and-comment process—problems which, she warned, acutely affected the FCC's handling of the net neutrality rulemaking:

> Since 1946, the Administrative Procedure Act has charged agencies making major policy decisions with the responsibility to open their process to the public. They are required to give "interested persons" an opportunity to voice their opinions, and only after considering these public comments may agencies proceed with proposed policies and adopt new rules.
>
> This system may have served Washington policymaking well for decades, but it is showing its age. In proceedings at this agency and others, the public is increasingly shut out of decision-making by the fraud that is flooding public channels for comment.
>
> You see this very clearly in the FCC's net neutrality proceeding. Last year, when the agency made the misguided decision to roll back its net neutrality rules, it did so based on a public record littered with problems. While millions of Americans sought to inform the FCC process by filing comments and sharing their deeply-held opinions about internet openness, millions of other filings in the net neutrality docket appear to be the product of fraud. As many as nine and a half million people had their identities stolen and used to file fake comments, which is a crime under both federal and state laws. Nearly eight million comments were filed from e-mail domains associated with FakeMailGenerator.com. On top of this, roughly half a million comments were filed from Russian e-mail addresses.

[13] The district court there also held that the FCC's server logs were exempt from disclosure under FOIA Exemption 7(E), 330 F. Supp. 3d at 334-35, but as noted the agency has not asserted that exemption here.

FCC 18-156 at 14 (statement of Commissioner Jessica Rosenworcel, dissenting); *see also* Jessica Rosenworcel, *Russians Are Hacking Our Public Commenting System, Too*, Washington Post (Mar. 6, 2018), https://wapo.st/2P0sGYW.

Finally, the FCC argues that the public interest is lessened in this case because there are "alternative sources" of information regarding the net neutrality rulemaking available, *i.e.*, investigations by government, academics, and the press regarding fake comments submitted to the FCC. FCC Memo at 22. That is an odd and novel proposition. One would have thought the array of investigations into the notice-and-comment process actually signals the intense public interest in getting to the bottom of what actually transpired. And to be sure, there are no "alternative sources" for the specific information The Times seeks here. The Times would not have pursued this Request for nearly two years and filed a lawsuit if there were.

The reality is that the FCC has consistently resisted demands to come clean about what happened during the net neutrality rulemaking. As Commissioner Rosenworcel warned: "It appears this agency is trying to prevent anyone from looking too closely at the mess it made of net neutrality. It is hiding what it knows about the fraud in our record and it is preventing an honest account of its many problems from seeing the light of day." That is a chilling warning—from a government official in a position to know. And it is entirely consistent with what is otherwise apparent from the record: there remain significant questions of immense public interest regarding the manner in which the FCC conducted the net neutrality rulemaking.[14]

[14] Should this Court find that Exemption 6 permits the FCC to withhold one piece of information but not the other (*e.g.*, originating IP addresses, but not User-Agent headers), the FCC must segregate and disclose the portions of the log that are not exempt. *See* 5 U.S.C. § 552(a)(8)(A)(ii)(II) ("An agency shall . . . take reasonable steps necessary to segregate and release nonexempt information.").

II.
THE FCC MUST DISCLOSE THE API PROXY SERVER LOG

The FCC's inexplicably belated disclosure that it possesses an API proxy server log containing both pieces of information sought by The Times simplifies this case. As set forth in the FCC's memorandum of law, The Times was originally told that the IP addresses and User-Agent header resided in two different logs; The Times accordingly proposed that the two logs be linked by having the FCC use a unique identifying number for each entry, allowing The Times to match the information in the first log to the same commenter's information in the second log. The FCC's eleventh-hour admission that it actually has the requested information in a single log moots the need for a "find-and-replace" method to link the two separate logs. It also moots the FCC's claim that The Times's Request calls for the creation of a new record.

The FCC has no reasonable basis for withholding the API proxy server log. Exemption 6 aside, the FCC offers a single reason it cannot produce the log: it is apparently not reasonably and precisely able to identify the log entries that correspond to the specific ECFS comments in the net neutrality proceeding. FCC Memo at 14-17.[15] The FCC concedes that it could develop a script to match comments from that proceeding to the logs based on their respective time stamps, but claims that would require the agency to go beyond what FOIA requires (*i.e.*, by conducting "research" and "answer[ing] questions disguised as a FOIA request," rather than performing a search) and that the results would in any event be "highly imperfect." *Id.* at 16-17; Scheibert Decl. ¶ 30. These assertions do not get the FCC anywhere near its burden of showing that it

[15] The FCC also says that the API proxy server log "contains other types of ECFS requests besides requests to post comments, such as requests to download comments." FCC Memo at 14. The Times does not interpret this to mean that the FCC is actually incapable of producing only those logs that correspond to POST requests.

cannot produce only those logs corresponding to the net neutrality proceeding. And even if they did, the proper course would be for the agency to disclose the entire API proxy server log (*i.e.*, for comments in all FCC proceedings) for the relevant period, not to withhold all of it.

As an initial matter, the FCC mischaracterizes the nature of the task before it. At least in the circumstances of this case, developing a script is functionally no different from designing and conducting a search for responsive records. Like a search, the purpose of such a script – which is essentially a set of commands to be executed by a computer program[16] – would be to identify agency records responsive to The Times's Request based on the content of those records. It does not require meaningful analysis of the data, nor does it entail the creation of a new record. To the extent that writing commands for a script may require an individual to exercise "judgment" (FCC Memo at 16), it is not materially different than creating parameters for a record search. An agency employee designing a record search must exercise judgment in selecting search terms, document custodians, and the universe of records to be searched. At least in this case, then, the script is the functional equivalent of a search. *See, e.g.*, *Schladetsch v. Dep't of Housing and Urban Dev.*, 2000 WL 33372125, at *3 (D.D.C. Apr. 4, 2000) (noting "that the programming necessary to instruct the computer to conduct [a] search does not involve the creation of a record").

Given that, it falls to the agency to show that developing the script in question would be "unreasonably burdensome." *Nation Magazine, Washington Bureau v. U.S. Customs Serv.*, 71 F.3d 885, 892 (D.C. Cir. 1995); *see, e.g.*, *Nat'l Day Laborer Org. Network v. Immigration and*

[16] *See* TechTerms, *Script*, https://bit.ly/2HRAITj ("A computer script is a list of commands that are executed by a certain program or scripting engine. Scripts may be used to automate processes on a local computer or to generate Web pages on the Web. . . . Script files are usually just text documents that contain instructions written in a certain scripting language.").

Customs Enforcement, 2017 WL 1494513, at *14 (S.D.N.Y. Apr. 19, 2017) ("When the reasonableness of search and production is questioned, the agency has the burden to produce a sufficient explanation as to why it would be unreasonably burdensome." (quoting *Tereshchuk v. Bureau of Prisons*, 67 F. Supp. 3d 441, 455 (D.D.C. 2014))) (internal marks omitted)). Generally that requires the agency to provide a "detailed explanation" of the time and expense of a proposed search. *Pinson v. Dep't of Justice*, 80 F. Supp. 3d 211, 216 (D.D.C. 2015) (quoting *Wolf v. Cent. Intelligence Agency*, 569 F. Supp. 2d 1, 9 (D.D.C. 2008)) (internal marks omitted). The FCC's papers are entirely silent on these matters. The agency gives no indication of the complexity, length of time, or cost involved in creating a script to match comments and logs based on timestamps.[17] At a minimum, the absence of this evidence makes summary judgment in the agency's favor inappropriate.

The agency also thoroughly fails to justify its assertion that the results of its script method would be "highly imperfect." Scheibert Decl. ¶ 30. The FCC speculates that because of the sheer number of comments made and the time gap between the comments and their respective logs, a "high confidence match (or even reasonable match)" between comments and logs will be "difficult to achieve." *Id.* However, the difficulty of this matching would presumably depend on the number and timing of ECFS comments submitted in other FCC proceedings (*i.e.*, those other than the net neutrality proceeding), and the agency says nothing about that. By The Times's own count, during the relevant timeframe (April 26 to June 7, 2017) just over three hundred comments and other filings (letters, petitions, etc.) were submitted in 46 other

[17] That omission is made more conspicuous by the FCC's representation that creating a different script – one to link the two sets of server logs originally sought by The Times – would "likely take over a week of staff time." Scheibert Decl. ¶ 33.

proceedings, compared to nearly five million in the net neutrality proceeding.[18] Likely some – and perhaps many – of those few hundred comments were submitted outside the periods of peak traffic in the net neutrality proceeding, which would greatly simplify the task of matching those comments to their respective log entries.

Put simply, the FCC needs to identify a relatively small number of entries irrelevant to net neutrality – a task achievable with minimum effort by matching the comments from the other proceedings with their IP addresses and User Agent headers.[19] However, should the Court determine that the FCC is not required to eliminate from the log those entries from proceedings other than docket 17-108, the entire log must still be produced to The Times. Apart from Exemption 6, the agency has not claimed that any parts of the log or log entries are exempt from disclosure. Thus, the proper course is for the FCC to disclose all of the log entries from the relevant timeframe, not to withhold all of them. *Cf. Am. Immigration Lawyers Ass'n v. Exec. Office for Immigration Review*, 830 F.3d 667, 670 (D.C. Cir. 2016) (finding "no statutory basis for redacting ostensibly non-responsive information from a record deemed responsive").

CONCLUSION

For the foregoing reasons, Plaintiffs respectfully asks this Court: (i) to deny FCC's motion for summary judgment and to grant Plaintiffs' cross-motion for summary judgment; (ii) to order the FCC to make public within 20 days, pursuant to 5 U.S.C. § 552, the API proxy server log entries for comments filed in the net neutrality proceeding; (iii) to award Plaintiffs the

[18] These figures were obtained by searching for FCC proceedings within the relevant date range at the ECFS search page (https://bit.ly/2qJzmRf) and counting comments in each proceeding.

[19] If there are in fact only several hundred log entries corresponding to comments submitted in other FCC proceedings, it is not clear why the agency cannot manually undertake the task of comparing the timestamps of those comments to the API proxy server log.

costs of this proceeding, including reasonable attorney's fees, as expressly permitted by FOIA, *id.* § 552(a)(4)(E); and (iv) to grant such other and further relief as the Court deems just and proper.

Dated: New York, NY
April 10, 2019

Respectfully submitted,

By: /s/ David E. McCraw

David E. McCraw, Esq.
Al-Amyn Sumar, Esq.
The New York Times Company
Legal Department
620 Eighth Avenue, 18th Floor
New York, NY 10018
Phone: (212) 556-4031
Fax: (212) 556-4634
mccraw@nytimes.com

John D. Clopper, Esq.
Clopper Law PC
43 West 43rd Street, Suite 95
New York, NY 10036
Phone: (347) 752-7757
jclopper@clopperlaw.com

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on this 10th day of April, 2019, a true and correct copy of the foregoing **MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT'S MOTION FOR SUMMARY JUDGMENT AND IN SUPPORT OF PLAINTIFFS' CROSS-MOTION FOR SUMMARY JUDGMENT** was filed with the Court through the electronic filing system, which will automatically serve electronic notice of the same on all counsel of record.

/s/ David E. McCraw